REMARKS

Claims 1-26 are presented for further examination. Claims 1, 2, 8, 25, and 26 have been amended. In the non-final Office Action mailed on December 3, 2008, the Examiner rejected claims 1-26 under 35 U.S.C. §102(b) or 103(a) as anticipated by U.S. Patent No. 7,325,246 (hereinafter "Halasz"). Applicants respectfully disagree with the bases for the rejection and request reconsideration and further examination of the claims.

Claim rejections under 35 USC §102(b) or 103(a)

Halasz relates to non-analogous subject matter and does not teach, suggest or disclose "(the authentication device) sending a message comprising ACCESS_ACCEPT information to said mobile host" and "said key-related information M1 used to obtain a key by the AP, and said message comprising the ACCESS_ACCEPT information is used to obtain the key by the mobile host" in claim 1.

Specifically, Halasz discloses architecture for **providing access to** an IEEE 802.1x network. A trust relationship is created between a switch of the network and an access point of the network such that the access point is authorized to communicate over the network. The trust relationship is then extended from the access point to a wireless client requesting connection to the network such that access to the network by said wireless client is authorized.

In contrast, the solution of claim 1 relates to **distributing encryption keys** in a Wireless Local Area Network (WLAN) by utilizing the process of authenticating a mobile host by an authentication device through an access point (AP).

In other words, according to the solution of amended claim 1, the process of encryption key distribution is combined with the process of mobile host authentication. When authentication fails, no encryption key is distributed; and when authentication succeeds, the authentication device sends key-related information M1 to the AP and sends a message comprising ACCESS_ACCEPT information to the mobile host, wherein the key-related information M1 is used by the AP to obtain **a key**, and the message comprising the ACCESS_ACCEPT information is used by the mobile host to obtain **the key**.

The Examiner asserts that Halasz teaches in col. 6, lines 34-58, that the authentication server (AS) sends an access-accept message comprising the key information and authorization state if authentication succeeds. After a careful review of Halasz, the Applicants note that Halasz does disclose in col. 6, lines 41-42 that the AS sends a session key and authorization state to the AP. However, Halasz does not disclose or teach the AS sending a message comprising ACCESS_ACCEPT information to the wireless client.

Further, the Examiner asserts that Halasz teaches at col. 4, lines 24-37, deriving for the wireless client in the same way a key is obtained for the AP during authentication at col. 3, lines 36-57. After a careful review of Halasz, Applicants also note that Halasz does describe at col. 3, lines 55-57, and col. 4, lines 31-33, that a message authentication check key exists between the switch and the AP, describes in col. 4, lines 33-34, and that a session key exists between the AP and the wireless client, and Halasz describes at col. 4, lines 28-31, that a session key is derived for the wireless client in the same manner as for the AP during its authentication process through the switch to the AS.

However, nowhere does Halasz disclose, teach, or suggest how to derive the session key, whether for the wireless client or for the AP.

Halasz further describes at col. 4, lines 34-37, that the session key for the wireless client uniquely encrypts the traffic from the wireless client to the AP, while the message authentication check key for the AP uniquely verifies the AP to the switch. That is to say, the session key and the message authentication check key are different ones used for different purposes.

In sharp contrast, according to the solution as claimed in claim 1, the AP obtains a key according to the key-related information M1, and the mobile client obtains the same key according to the message comprising ACCESS_ACCEPT information. That is to say, the AP and the mobile host obtain the same key in different ways.

Based on the above, Applicants respectfully submit that the solution of claim 1 is completely different from that disclosed by Halasz. Claim 1 is thus not anticipated by Halasz in the sense of 35 U.S.C. 102(b).

The Examiner also rejects claims 2-5, 10, 15, 20, 25 and 26 under 35 U.S.C. 102(b) as anticipated by Halasz.

Applicants respectfully submit that dependent Claims 2-5, 10, 15 and 20 are also not anticipated by Halasz for the features recited therein as well as for the reasons why claim 1 is allowable as discussed above under 35 U.S.C. 102(b). In addition, at least for reasons similar to those for claim 1, amended independent claims 25 and 26 having features that correspond to those of claim 1 are not anticipated by Halasz under 35 U.S.C. 102(b).

The Examiner further rejects claims 6-9, 11-14, 16-19 and 21-24 under 35 U.S.C. 103(a) as unpatentable over Halasz and further in view of U.S. Patent No. 6,853,729 (hereinafter "Mizikovsky"). (Applicants have amended claim 8 to correct a minor typographical error; no new matter has been added.)

As stated above, Halasz does not disclose, teach, or suggest the limitations "(the authentication device) sending a message comprising ACCESS_ACCEPT information to said mobile host" and "said key-related information M1 is used to obtain a key by the AP, and said message comprising the ACCESS_ACCEPT information is used to obtain the key by the mobile host" in claim 1 of the present application. In addition, there is no suggestion in Mizikovsky to combine such limitations in claim 1 with the limitations in claims 6-9, 11-14, 16-19 and 21-24 and further in the intermediate claims, if any, to reach the solution recited in claims 6-9, 11-14, 16-19 and 21-24. At least for these reasons, claims 6-9, 11-14, 16-19 and 21-24, which are dependent from claim 1, either directly or indirectly, are not suggested and are patentable over Halasz and further in view of Mizikovsky under 35 U.S.C. 103(a).

In view of the forgoing, the Applicants respectfully submit that based on the above comments and the corresponding amendments, the entire application is now in condition for allowance, which is respectfully requested. In the event the Examiner disagrees or finds minor informalities that can be overcome by telephone conference, the Examiner is urged to contact the undersigned by telephone at (206) 622-4900 in order to expeditiously resolve prosecution of this application. Consequently, early and favorable action allowing these claims and passing this case to issuance is respectfully requested.

The Director is authorized to charge any additional fees due by way of this Amendment, or credit any overpayment, to our Deposit Account No. 19-1090.

Respectfully submitted,

SEED Intellectual Property Law Group PLLC

/E. Russell Tarleton/
E. Russell Tarleton
Registration No. 31,800

ERT:alb

701 Fifth Avenue, Suite 5400
Seattle, Washington 98104
Phone: (206) 622-4900
Fax: (206) 682-6031

470061.401USPC / 1340885_1.DOC